Encryption and DropBox: Comparing TrueCrypt and BoxCryptor

Wednesday, January 4th, 2012

If you're a DropBox[1] user, you may have heard about the security weakpoints associated with their cloud storage service (or any such service):

1. DropBox has had security issues[2] that left users' information exposed to hackers for hours at a time. Could it happen again? Certainly.
2. DropBox staff have the ability to access your files[3] without your knowledge. They have acknowledged that essentially the only thing between their staff and your data are internal company policies. This is much weaker than zero-knowledge systems like SpiderOak, where it is not even technically possible for staff to access users' files without the user's key.

Even knowing these weaknesses, I use DropBox anyway. Having access to *some* (not all, obviously) potentially sensitive files on multiple computers/phones is helpful enough for me to find some way to mitigate the security risks.

It's important to note that if you're putting sensitive files on DropBox purely as a backup solution, you should just stop. Find some other way to back those files up. But if, like me, you find it extremely helpful to have access to certain moderately sensitive files from multiple devices, you should find a way to add a layer or two of security to those files before storing them on a cloud service like DropBox.

There are two good ways that I have found to do this. Both are free, and neither involve sending any of your data or keys to an additional third party—all the magic happens on your computer or device. However, there are trade-offs associated with each.

The TrueCrypt Option

The most commonly offered solution is to place your sensitive files in a TrueCrypt[4] volume and save that volume file into your DropBox.

1. http://dropbox.com
2. http://techcrunch.com/2011/06/20/dropbox-security-bug-made-passwords-optional-for-four-hours/
3. http://www.wired.com/threatlevel/2011/05/dropbox-ftc/
4. http://www.truecrypt.org

Pros:

- TrueCrypt is open source, making it the most trustworthy and future-proof option
- For extremely sensitive info, TrueCrypt allows you to maintain plausible deniability[5].

Cons:

- There is currently no way to use or access TrueCrypt volumes on your phone. This is true both for iPhones and Android phones.
- TrueCrypt volumes need to be given a fixed size at the time of creation, forcing you to guess how big it'll need to be in the future and usually resulting in wasted space.
- You need to be careful not to have the volume "mounted" on more than one computer at a time to avoid corrupting it. Because there's nothing to prevent you from doing this, you can easily end up corrupting the volume or creating a lot of large "conflict copies" of the volume by accident if you forget this.
- Because DropBox can't back up changes to any of your encrypted files until you actually unmount the whole volume, you have to remember to unmount it periodically, which can be cumbersome.

The BoxCryptor option

BoxCryptor[6] is a newer solution that works by encrypting individual files on your computer, before they are sent to DropBox. Like TrueCrypt, the software runs on both Windows and Mac OS.

Pros:

- BoxCryptor has an Android and an iPhone version of their software, making it possible to access encrypted DropBox files from your phone.
- The software has limited compatibility with the open-source EncFS encrypted file system, making it at least somewhat future-proof

5. http://www.truecrypt.org/docs/?s=plausible-deniability
6. http://www.boxcryptor.com/

- File-level encryption makes it much less clumsy to use, and allows DropBox to sync encrypted files just as seamlessly as normal files, and without additional likelihood of conflicts where multiple computers are involved.

Cons:

- The iPhone app is $8 for non-commercial use. This seems stupidly high, considering the Windows and Mac versions are free and they have no back-end infrastructure to maintain.
- No form of plausible deniability is available in either the desktop or mobile versions of the software.
- BoxCryptor is not open-source, so ultimately your trust in the software comes down to your faith in Robert Freudenreich[7]'s ability to correctly implement the security algorithms, to keep maintaining the software, and not to spy on his users. I'm not saying he's untrustworthy, just that non-open software comes with risks and weaknesses. The security community at large does not have a way of thoroughly and independently evaluating the software, and that represents a security weakness, for one. Furthermore, if Robert or his company lose interest in the software (which can happen for any of a dozen reasons) you will need to take notice and migrate to another solution before you lose all ability to support the now-defunct software.

Responses

> I'm still debating this quandary.
>
> (Conversation Communications, October 23, 2012)

> It is possible to access TrueCrypt volumes on Android. There is an app called EDS which lets you open TrueCrypt volumes, even ones in DropBox.
>
> I believe I saw a similar app for iOS devices.
>
> (Teddy, December 06, 2012)

7. http://blog.robert.freudenreich.eu/